PERGAMON Computers and Mathematics with Applications 37 (1999) 85–87

An International Journal
computers & mathematics
with applications

Broadcasting Cryptosystem in Computer Networks

HORNG-TWU LIAW
Department of Information Management
Shih Hsin University, Taipei, Taiwan 116, R.O.C.

(Received May 1995; revised and accepted June 1998)

Abstract—A cryptosystem which can securely broadcast secret messages in a public access distributed system is proposed. Comparing with the existing broadcasting schemes, this scheme always requires fewer broadcasting messages. Furthermore, when a new user is inserted into the distributed system, the corresponding secret and public keys can be determined without changing any existing keys.

Keywords—Broadcasting, Distributed system, Public-key cryptosystem, Security.

INTRODUCTION

Due to the fast progress of computer communication networks and popularity of distributed processing systems, sharing of remote expensive resources becomes a reality. However, sharing makes it quite difficult for ensuring that unauthorized persons do not have access to either information stored in the system or messages during transmission over the network. All the methods before [1–3] need a large amount of broadcasting messages and have great difficulty in handling new users. In this paper, a cryptosystem to overcome these problems is proposed.

BROADCASTING SCHEME

Since this proposed scheme is based on the RSA public key scheme [4] and a conventional cryptosystem such as DES [5], their schemes are introduced first. With the RSA scheme, there exist two keys, d and e, that work in pairs for decryption and encryption, respectively. The starting point in finding keys for this scheme is to select a secret pair (p, q) of large prime numbers, and make $m = p \cdot q$ public. Besides, the Euler $\Phi(m) = (p-1) \cdot (q-1)$, and let a small odd integer e be chosen so that e is relatively prime to $\Phi(m)$. Then, select d such that $e \cdot d \equiv 1 \bmod \Phi(m)$. A plaintext message M is encrypted to ciphertext C by $C = M^e \bmod m$, and then the plaintext is recovered by $M = C^d \bmod m$. Because of symmetry in modular arithmetic, encryption and decryption are mutual inverse and commutative. Therefore, $M = C^d \bmod m = (M^e)^d \bmod m$. In this paper, in order to ensure the security of our scheme, we modify the RSA public key scheme. Let $p = 2p' + 1$ and $q = 2q' + = 1$ where p', q' are primes. Define $\lambda(m) = \text{lcm}(p-1, q-1)$ and

The author would like to thank the referees for their valuable comments and suggestions.

0898-1221/99/$ - see front matter Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX
PII: S0898-1221(99)00078-4

select d such that $e \cdot d \equiv 1 \bmod \Phi(\lambda(m))$. On the other hand, with the DES scheme, a master key MK is used as the encryption/decryption key. Therefore, $M = D_{\mathrm{MK}}(E_{\mathrm{MK}}(M))$, where $E(\cdot)$ and $D(\cdot)$ denote the enciphering function and deciphering function, respectively.

Consider a distributed system consisting of n users denoted by $U_1, U_2, \ldots, U_n$. In the network, all users can directly communicate with each other, that is, the network is fully connected in the way that two users can directly communicate with each other. Besides, it is assumed that there is a central authority server (CAS for short) in the distributed system.

Initially, the CAS assigns user U_i of the distributed system two secret keys t_i and K_i, and a public key $f(t_i)$. Assume that all the secret keys are known only to the CAS and user U_i. Besides, all the keys are constructed as follows:

$$t_i = P_i, \quad f(t_i) = t_i^e, \quad \text{and} \quad K_i = K_0^{t_i} \bmod m,$$

where P_i is a prime number, and K_0 is a secret key possessed by the CAS.

In this scheme, assume $P_1, P_2, \ldots, P_h$ are h distinct primes, where h is large enough to use in our assignment. In the following, a secure a broadcasting mechanism for distributed systems is presented. This scheme essentially consists of two phases.

1. In the first phase, the CAS constructs two public keys $f(B_i)$ and PK_i for sender U_i.
2. In the second phase, U_i decrypts the master secret key MK_i and then broadcasts the ciphertext C.

Without loss of generality, let U_1 be the sender, $U_2, U_3, \ldots, U_a$ be the legitimate recipients, and $U_{a+1}, U_{a+2}, \ldots, U_n$ be the illegitimate recipient.

Phase 1: (Construct two public keys for the sender.)

Step 1: (Broadcasting request from the sender.) U_1 tells the CAS that he wants to broadcast a message M to $U_2, U_3, \ldots, U_a$.

Step 2: (Construct two public keys $f(B_1)$ and PK_1 by CAS.)

$$B_1 = t_2 \cdot t_3 \cdot \ldots \cdot t_a, \qquad f(B_1) = B_1^e,$$
$$\mathrm{MK1} = K_0^{B_1} \bmod m, \qquad \mathrm{PK}_1 = E_{t1}(\mathrm{MK}_1).$$

Phase 2: (Compute the encryption key MK_1 and broadcast the ciphertext C.)

$$\mathrm{MK}_1 = D_{t_1}(\mathrm{PK}_1), \qquad C = E_{\mathrm{MK}_1}(M).$$

Note that, in our scheme, the encryption key e is secret and is possessed by the CAS. However, the decryption key d is public. The value $f(t_j)$ for each user U_j is public and can be used to derive the key of the sender in the distributed broadcasting system. It turns out that the value $(f(B_i)/f(t_j))^d \bmod \lambda(m)$ is equal $B_i/t_j \bmod \lambda(m)$ if and only if U_i is the sender and U_j is the legitimate recipient. The following theorem establishes this fact.

THEOREM 1. *Let U_i and U_j be two users in a system. If U_i is the sender and U_j is the legitimate recipient, then $(f(B_i)/f(t_j))^d \bmod \lambda(m) = B_i/t_j \bmod \lambda(m)$.*

PROOF. Since U_i is the sender and U_j is the legitimate recipient, let $B_i = r \cdot t_j$, where $r = B_i/t_j$. Then, $f(t_j) = t_j^e$, and $f(B_i) = B_i^e = (r \cdot t_j)^e$. Therefore, we have

$$\begin{aligned}
\left(\frac{f(B_i)}{f(t_j)}\right)^d \bmod \lambda(m) &= \left(\frac{(r \cdot t_j)^e}{t_j^e}\right)^d \bmod \lambda(m) \\
&= r^{e \cdot d} \bmod \lambda(m) \\
&= r^{e \cdot d \bmod \Phi(\lambda(m))} \bmod \lambda(m) \\
&= r \bmod \lambda(m) \\
&= \frac{B_i}{t_j} \bmod \lambda(m).
\end{aligned}$$

∎

Therefore, the legitimate recipient U_j can derive the secret key MK_i came from the sender U_i and then obtains the broadcasting message M by employing the following decryption phase.

Decryption phase: (Reconstruct the encryption key MK_i and decrypt the broadcast message M.)

$$\begin{aligned}
\mathrm{MK}_i &= K_0^{B_i} \bmod m \\
&= \left(K_0^{t_j}\right)^{B_i/t_j} \bmod m \\
&= \left(K_0^{t_j}\right)^{B_i/t_j \bmod \lambda(m)} \bmod m \\
&= K_j^{(f(B_i)/f(t_j))^d \bmod \lambda(m)} \bmod m \\
&= K_j^{(f(B_i)/f(t_j))^d} \bmod m \\
M &= D_{\mathrm{MK}_i}(C).
\end{aligned}$$

SECURITY ANALYSIS

The legitimate recipient U_j can drive the message M came from the sender U_i by using the decryption phase proposed above. However, it is infeasible to derive the secret key MK_i by only knowing the public keys of the sender U_i for any illegitimate recipient, because the security of our scheme is the same as the RSA public key scheme, which is strongly believed to be computationally difficult to attack. Moreover, this proposed scheme is secure on attacks by an intruder using the following approaches.

1. Find the secret key MK: in this case, it is assumed that an illegitimate recipient is trying to evaluate the secret key MK. Since an intruder does not satisfy Theorem 1, he cannot employ the decryption phase mentioned above.
2. Obtain the secret keys K_i and t_i only known by user i: the intruder may come from those legitimate recipients, since there is no information available to compute the secret keys K_i and t_i. Hence, this protocol also can protect the security of K_i and t_i.

From the above discussion, this proposed protocol is secure since it can prevent the secret keys MK_i, K_i, and t_i from being disclosed.

CONCLUSIONS

A secure broadcasting mechanism in distributed systems has been proposed. It is ensured to prevent the attacks and effectively reduced the broadcasting messages generated by the sender, hence this scheme is feasible for broadcasting messages in a distributed system. Besides, no modification of the secret and public keys is necessary when a new user is inserted into the distributed system, or an existing user is removed from the system, which is needed by almost all past broadcasting schemes.

REFERENCES

1. C.C. Chang and T.C. Wu, Broadcasting cryptosystem in computer networks using interpolating polynomials, *Computer Systems Science and Engineering* **6** (3), 185–188, (1991).
2. G.H. Chiou and W.T. Chen, Secure broadcasting using the secure lock, *IEEE Trans. Software Engineering* **15** (8), 929–934, (1989).
3. W.G. Tzeng and M.S. Hwang, A conference key distribution scheme for multilevel security, In *Proceedings of the Fifth National Conference Security*, May 1995, Taiwan, pp. 47–52.
4. R.L. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signature and public-key cryptosystem, *Communications of the ACM* **21** (2), 120–126, (1978).
5. D.E.R. Denning, *Cryptography and Data Security*, Addison-Wesley, Reading, MA, (1982).